

# **FEDERAL WIRELESS POLICY COMMITTEE**

## **Federal Functional Requirements for Commercial Wireless Services**

REVISION December 11, 2001

Send Comments to [mkruhl@alpha.ncsc.mil](mailto:mkruhl@alpha.ncsc.mil)

## 1. INTRODUCTION

What does the Federal Government want from the wireless communication industry as a customer of that industry's products and services? How can the government tap the market dynamics of this burgeoning industry to enhance services and reduce costs? This document seeks to answer these questions. The requirements discussed here apply not just to the telecommunications industry, as the Federal Government's supplier of wireless goods and services, they include also a forecast of policy, economic and managerial requirements upon Federal Chief Information Officers (CIOs) and agencies that lie just over the horizon. Thus, this document is intended as much for Federal agency officials as for the private sector telecommunications industry.

The Federal Government is not a single enterprise purchaser of wireless communication goods and services. Acquisition is done by many agencies each trying to support their unique missions. However, there are certain common issues and needs, some of them government unique, which form the emphasis of this document.

In laying out these requirements, commercial wireless communications (herein referred to as wireless) is an integral part of the Government's telecommunications infrastructure. It is not a special application interfacing with wireline networks, but is an integral part of future national and international networks. Wireless communications are becoming so integral to the telecommunications infrastructure that, ultimately, information systems designers will no longer need to concern themselves with whether end users are on wired local area networks (LANs) or unwired client devices. This places wireless as a major component and concern as addressed by the President's Commission on Critical Infrastructure.

One of the unique qualities of the Federal Government is its sheer size and scope, including its millions of employees and uniformed servicepersons. They are spread from the sands of Middle Eastern deserts, across and under the oceans, through the skies, and deep into the national forests and parks, the Indian reservations, and the inner cities of America. Federal workers staff VA hospitals, assist farmers, inspect waterways, facilitate Social Security payments, conduct court cases, fight terrorism, and collect customs duties, in addition to defending the Nation abroad.

The government's future use of wireless will be inextricably tied to the cost of these services and to the value it brings to our missions. Replacing or modernizing the government's huge inventory of systems can only be accomplished if the value is clear and the acquisition, maintenance, subscription and operational costs can be justified.

Today many of these workers are tethered to wired workstations and telephones in government owned or leased office space. Tomorrow most will be wireless, untethered, and operate in new settings in addition to the conventional spaces they occupy now. The impact will be both improved services and more efficient operation.

## **2. SCOPE**

The federal user requirements identified in this document encompass a broad array of user needs in the civil and defense agencies. These requirements are largely common with those of the business community, but some are unique. The scope of wireless in this document includes licensed and unlicensed *commercial* products and services, which include:

- Cellular
- Personal Communications Service (PCS)
- Mobile Satellite Service (MSS)
- Specialized Mobile Radio (SMR)
- Wireless Wide Area Networks (WWAN)
- Wireless Local Area Network (WLAN)
- Wireless Private Branch Exchange (PBX)
- Wireless Local Loop (WLL)
- Paging.

The scope does not consider commercial TV, custom military radio, private land mobile radio, or point to point satellite trunking.

## **3. BACKGROUND**

The requirements outlined in this document revise those developed in 1994 under the Federal Wireless Policy Committee (FWPC) on the basis of trends and policy decisions in the federal government. Recent decisions in Congress and the Federal Communications Commission have redirected the development and deployment of dedicated Federal wireless services using federal spectrum to commercial leased systems. The Congressional actions include the Clinger Cohen Act (also known as the Information Technology Reform Act) and the Telecommunications Act of 1996. These two actions taken by Congress have caused a significant impact in the areas of telecommunications and information technology. Specifically, these acts encourage the procurement of commercial off-the-shelf (COTS) products and services instead of custom products and government unique developments.

The requirements in this document have come from numerous government agency members that participate in the Federal Wireless Users Forum (FWUF), including user workshops, and the Federal Wireless Policy Committee (FWPC).

The FWPC was established in November 1993 with membership of all major federal agencies that have operational, procurement, or policy interests in the development of new wireless Personal Communications Services and other emerging technologies. The FWPC is chaired by the National Telecommunications and Information Administration (NTIA) and vice chaired by the Office of the Manager, National Communication System (OMNCS). The FWPC Chairperson also serves as the Assistant Secretary of Commerce for Communications and Information who is the principal advisor to the President on telecommunications policy.

The FWUF, a forum that provides guidance to the FWPC, was established for government personnel to exchange ideas through interaction with commercial service providers and developers of emerging wireless technology. The FWUF was established by the President as a result of recommendations of the President's National Security Telecommunications Advisory Committee (NSTAC) in their September 5, 1992 Report. The FWUF sponsors workshops for the government and commercial entities to come together and discuss requirements and commercial solutions.

#### **4. THE WIRELESS VISION**

Currently new satellite and terrestrial wireless systems are being built that, together with premises based wireless capabilities, are transforming the communications landscape. Already, the global wireless market is approaching a Trillion dollars. In North America alone, \$100 Billion has been invested in wireless infrastructure to give location independent communications to people on the move. In view of the changes in global commerce and transportation, and the impacts of the Internet and electronic commerce, one can see clearly that the enormous changes coming in wireless communications are being market driven.

By the end of the next quarter century, the already ubiquitous cell phones and pagers will have given way to similar sized devices that provide full data capabilities and video conferencing capabilities. The public safety sector will have migrated to fully digital and interoperable wireless systems; and many Federal agencies will routinely conduct official Government business with their mission partners over wireless communications links.

For much of the Federal Government, the coming years will bring a heightened emphasis on Service to Citizens. As the American population increasingly carries portable telephones and personal computer devices, "smart cards" or their successors for access and transactions, and is accustomed to conducting personal and employer business activities without regard for day or hour, Federal agencies are likely to demand similar services. One way is to find new cost effective ways to bring Government to people instead of making people come to fixed Government offices during "business hours". Whether it is mobile van offices at shopping centers or similar strategies, wireless communications will be one of the keys to success.

For the Government's Information Technology (IT) community, the opportunities ahead include merging voice and data, sharing high-speed wireline networks, and integrating those networks with wireless services from multiple providers nationally and internationally.

The coming wireless era will bring ubiquitous paging capabilities that combine lifetime number assignments and national and international roaming, to provide Federal employees the ability to be contacted anytime or anywhere. They will be contactable by

their supervisors and co-workers, their clients, other mission partners in state and local governments, and private citizens. This ease of reach will create major new issues on workforce management, employee relations, and systems design and administration, as well as policies and procedures for the conduct of mission business with the public.

The future application of wireless technology will not be limited to civil agencies. The Joint Vision 2010, for example, shows wireless solutions being applied by the military as well. Mobile Satellite, PCS and WLANs will be extensively deployed to support military operations nationally and internationally.

New wireless technology will enable Federal employees to pick up their voice mail messages and read their last night's Internet, Intranet, and Extranet mail messages while riding the Subway to work. They will scan the morning's news on their government issued personal communications device, which will operate seamlessly as they move from the Subway into the office building.

## **5. REQUIREMENTS IMPLICATIONS**

### **5.1 Policy, Economics, and Information Management**

This vision of this future wireless technology raises intriguing policy questions regarding priority communications, personnel management, physical deployment of workers, workplace design, and customer relations. Soon such issues will be prominent on the meeting agendas of the Government's CIO Council.

New issues in information management must be considered. Wireless capabilities will affect requirements for managing information created and stored in wireless devices, and how data is integrated into agency information systems and record keeping systems. These future system designs for information storage in wireless "clients" where that information is a portion of an agency's information assets will be affected by economic and technical considerations.

Federal government wireless solutions must consider significant economic implications such as pricing models, billing and accounting, and charge back mechanisms. Pricing models will drive budgeting, and vice versa, and the Federal Government's budgetary structures and processes may be incompatible with service providers' pricing schemes. The Government must posture itself to use its aggregated purchasing power to obtain compatible pricing models and quantity pricing for the volumes required by the Government. Similar issues relating to lease plans for subscriber devices are likely. In order for the Federal government to fully utilize commercial wireless, these services must be cost effective.

In all probability, the Government will not need billing and accounting support from providers that is significantly different from what is offered large multinational enterprise

customers. However, the agency structure of the Federal Government may add some unique dimensions to the customary provider billing arrangements such as charge backs for services that are acquired on a multi agency basis.

The most significant policy, economic, and information management requirements are those associated with the protection of Government assets and personal privacy. These protection needs extend beyond the mobile terminal into many levels of infrastructure protection including agency level, some at the government wide level, and some at the level of the national and international providers of wireless services. Wireless cannot be thought of as just cellular phones and pagers, where security means protection against fraudulent use and eavesdropping. The future security requirements will include all of those currently associated with wire network information systems, plus all issues arising from wireless mobile communications from individuals in and away from the office. Addressing security requirements will be a major priority due to the additional exposure and vulnerability associated with wireless technology.

## **5.2 Performance and Technology Issues**

The following sections deal in some depth with many projected requirements concerning performance and technology. The following are selected issues that identify future applications and needs.

- **Multimedia and Bandwidth, and Multi-Use** – Wireless technology development will include options that provide expanded bandwidth for mobility and flexibility. Traditional voice and data applications will become integrated as the cell phone and the laptop computer merge and blend functions.
- **Roaming and International Support** - The Federal Government's mission requires global coverage. Furthermore, these international requirements will lead Federal agencies to obtain subscriber services and devices for both inside and outside the territorial United States.
- **Interoperability** – It is apparent that digital networks will dominate business communications in the future. It is essential that the wireless services of tomorrow support interoperation among the many different networks (commercial and private/government), associated technologies, and service providers.
- **Security and Priority Treatment** – Priority treatment and Security continue to be critical, and in some cases, unique requirements of the federal user. Accommodating these requirements within the framework of commercial services and products is key.

## 6. FUNCTIONAL REQUIREMENTS

### 6.1 General

These federal user requirements for wireless products and services are generally characterized as Digital, Ubiquitous, Interoperable, Transparent, and Secure (DUIITS) as defined below.

- **Digital** - service performance supported by high performance digital communication link protocols. Such protocols enable better radio link communication performance and the addition of higher layer services to support data, security, and enhanced network features.
- **Ubiquitous** - support for wide coverage areas. Ubiquitous service requirements include geography, compatibility, and service provisioning. Each of these must be present to support mobile users of one or more air interface (radio) technologies.
- **Interoperable** - the direct compatibility between user and service infrastructure as well as extending features across the service provider and local network domains. Interoperability can include multi-mode operation and/or service interworking.
- **Transparent** - the maintenance of service features, performance, and operation to the user across service and network boundaries.
- **Secure** – the suite of information security features provided by the network and/or available in the user terminal. Security features include the traditional confidentiality, authentication, integrity, availability, and accountability described in the section on security that follows.

These features are common to the needs of the large business communities except that the scope of government needs are often broader and the impact more urgent. Government users require voice, data, fax, paging, imagery services, e-mail, file transfer, Internet access, Intranet access, remote computing and more for diverse applications. Security features are required in most applications. During periods of natural disasters and crisis it is especially important that resources be available and readily configurable both nationally and internationally.

These functional requirement issues extend beyond the scope of domestic activity to international activity. The mission of many federal users requires equipments and services that operate transparently as part of a global service. These general requirements are expanded below.

## **6.2 Common and Standardized Radio Interface and Protocols**

Standardized radio protocols and interfaces are needed for federal users to achieve DUITs services. Ideally the development of a single national or international standard would facilitate this objective. Unfortunately today's wireless offerings and industry competition drive technology development that impedes these objectives. The manufacturers and industry standards bodies are encouraged to move toward a unifying set of standards while providing backward compatibility for legacy services during a transition.

In the absence of a single standard, support for Ubiquity, Interoperability and Transparency may be accomplished for federal users with a mixture of strategies as listed below.

- The federal community selects a particular technology that supports their mission over the service coverage area. While this approach satisfies a requirement on a local or regional basis, such a strategy is a piecemeal approach that limits coverage and competition.
- The federal community uses multi-mode terminals for service that is provided in the areas where multiple technologies are deployed. While this strategy is also a local or regional solution, it could provide the federal user a competitive environment for equipment and service providers.

## **6.3 Multi Band Multi Mode Terminals**

More than one service may be required to support DUITs. Ideally, a mixture of mobile satellite, PCS/cellular, wireless PBX, WWAN, WLAN, and paging, are desired. While all combinations are neither required nor practical some combinations have been identified and others may exist as shown below:

- Mobile Satellite Services/PCS/Cellular - Many government missions require operating in both high-density urban and low-density remote coverage areas where the integration of these services would add significant value to the user.
- Cellular/Wireless PBX – Offering roaming between a cellular/PCS system and an unlicensed campus or office system would offer cost-effective solutions for many government missions.
- Point-to-Point/Cellular/SMR Many government users have requirements for extending the service coverage provided by cellular/PCS or SMR systems to include a simple point-to-point (radio to radio) mode for highly localized operation.

## 6.4 Applications & Services

The combinations of services and applications are too broad to describe completely. In general the applications and services coincide with the trend within the government, and the commercial sector, to use new information technology services to enhance operation and improve efficiency. Federal use will grow with the availability of service and bandwidth. The required data rates will vary with service offerings and application. The high-end data rate will depend largely on the technology, utility, and timeframe. A sampling of government application and service needs are presented below.

- **Circuit Mode** - Circuit mode services provide a dedicated traffic channel for traditional voice telephony, circuit mode data, facsimile, video and multiplexed voice/video/data applications. Current data bandwidth requirements of approximately 9.6kbps are expected to expand to megabits per second and beyond as new applications are developed. The mobile office application is a typical scenario where field services are provided in temporary or mobile configurations. The 2000 census was one such application.
- **Interactive Mode** - Interactive mode services include terminal/server applications or Internet applications where connection based packet services would typically be used. Bandwidths ranging from 4.8kbps up to megabits per second would be required depending on the application and the service. The wireless office or the mobile field agent would likely use such a service.
- **Transaction Mode** - Transaction mode service includes short message, e-mail, vehicle location, material tracking, paging, and dispatch operations. Such applications would typically be supported by connectionless packet based services at a variety of data rates typically below 9.6kbps. Such services are used in the public safety community.
- **Transparent Data Capabilities** – Transparent data connections on wireless networks are required for end-to-end security for sensitive and classified voice and video applications. Such applications required fixed end-to-end delay, low latency (<200msec), and the ability to select and configure intermediate networks services for an end-to-end transparent service. Such services would be used throughout the government for voice, video, and data security applications. Data rates ranging from 2.4 kbps to megabits per second are required depending on the wireless technology and the application.

## 6.5 Network Services

Network services play an increasingly greater role to the wireless user. Network services are required to interoperate with the diverse network elements and to support the user service. The interaction of wireless and wired services should be complementary. It is expected that the normal network services planned for commercial applications will also be available to the government user. The following examples highlight some network

services of special interest to government applications that should operate consistently across wireless and wired boundaries:

- **Interworking**-A means of supporting communications interactions between entities in different networks or systems. An example is a transparent Network-to-Network Interface across a wireless network to the PSTN.
- **User Identity Module (UIM)**-A standard device or functionality providing secure procedures in support of personnel and terminal mobility, registration, authentication, and privacy for wireless access to PCS, which may also be used to facilitate other services (e.g. banking).
- **Personal Mobility**-The ability of a user to access telecommunication services nationally and internationally at any terminal on the basis of a personal identifier (e.g. UIM), and the capability of the network to provide those services according to the user's service profile.
- **Terminal Mobility**-The ability of a terminal to access services from different locations nationally and internationally, and the ability of the network to identify and locate that terminal.
- **In-Call Modification**-The ability of a user to indicate to the network how to handle incoming calls according to certain parameters such as the originator of the call, the time of day and the nature of the call.
- **Call Associated Signaling (CAS)**-The signaling required to manage a bearer service between two end points such as call origination, call delivery, and handover.
- **Non-Call Associated Signaling (NCAS)**-Signaling that is independent of an end-to-end bearer connection such as registration, authentication, and validation.
- **Handover**-This is the action of switching a call in progress from one cell to another or between radio channels in the same cell. Handover is used to allow established calls to continue when mobile stations move from one cell to another or as a method to minimize co-channel interference.
- **Roaming**-The ability of a user to access services in an area other than where the user is subscribed.
- **Government Emergency Telecommunications Service (GETS)**- A service provisioned within the wired network to assure call completion.
- 
- **Priority Service** – This includes priority access to guarantee or enhanced access to wireless services, priority treatment through the network(s), and priority egress to ensure call completion to either a wireline or wireless terminal device.
- **Alternate Voice and Data Services** – The ability to switch bearer services within a call such as the transition from voice to data needed for secure voice and video applications.
- **Conferencing Services** – Access to conference features within and across networks.
- **Off-hook (ring down) services** – The ability to establish and have in place end-to-end connections that can be invoked simply by going off hook.

- **Broadcast/Dispatch services** – The ability to connect users within and across networks in a broadcast mode where one user talks to many or, in a net broadcast mode, where any one of the users can broadcast to all.

## **6.6 Transparent Network Interworking**

Support for Ubiquity, Interoperability and Transparency requires the user services be supported across network and carrier boundaries. The services that originate in one carrier's wireless network will often be connected through the PSTN, the Internet, or to another carriers wireless network. The services and applications identified above must be supported transparently through a mix of networks if it is satisfy these requirements. Seamless, transparent service across the network boundaries is essential to this capability. These features are emerging in commercial services and the need is common to government and commercial users.

## **6.7 Terminal Features**

Some government users are likely to have special requirements such as ruggedized products for military, law enforcement, emergency medical, and park-service applications, Electromagnetic Interference and Compatibility (EMI/EMC), and customized maintenance support.

## **6.8 Acquisition and Billing Requirements**

Many government agencies will require special acquisition and billing features associated with wireless service. Government users will want access to products, services, and special service packages similar to those offered to the commercial customer while maintaining the ability to bundle acquisition and billing at a department or agency level. Accountability for service will vary with agency and by acquisition mechanism. Service billing should be capable of providing accounting details at all levels of the agency or department in a form suitable for automation.

As implied above, many Federal employees in the years ahead will be issued communication devices to be used away from the normal workplace, or in a mobile workplace, that (a) will be either entirely wireless or both wireless and wire line, and (b) will be capable of being used for both business and personal purposes, as is the case with today's voice telephone systems. Conversely, employees will be able to use their personally obtained devices for business purposes, as is the case today with employees making business phone calls at their home instruments, or using their personally owned home computers to access government e mail or other systems. What the years ahead will bring is a greater degree of this duality, affecting many more employees than is the case today.

In recognition of the multi-use capability of tomorrow's systems and devices, the Government may wish to consider requiring devices to be equipped with a "Business/Non-Business" switch, or its equivalent, and requiring service providers to accommodate a corresponding alternative billing capability for subscriber usage, invoked at time of usage for services whose costs are usage based. Other requirements may focus on "acceptable use," or how devices and systems are configured for authentication and encryption. It might be in the Government's best interests to seek to replace today's practices of having Federal employees reimburse agencies for personal use of Government facilities and services with strategies based on service provider alternative billings.

## **6.9 Priority Requirements**

**6.9.1 Priority Service** - Wireless systems should provide a uniform, nationwide priority service to authorized federal agencies during emergencies when wireless networks become congested. A nationwide priority service is needed to allow authorized users access to wireless service when they need it, regardless of origination or termination location. A uniform service will provide a capability that is interoperable with existing wireless users infrastructure and activate the service identically across the nation. In other words, the priority scheme should be available to any authorized users on a standard terminal with the same service activation process used throughout all regions of the country. In addition, these standardized services should be extendable to international applications where feasible.

The wireless priority treatment must be compatible with current and future authorized federal capabilities, should not preempt nor affect calls in progress, and provide authorized priority users preferential treatment for any priority calls (i.e., voice, imagery or data attempts) via wireless networks. Priority capabilities within wireless networks must provide preferential treatment through all components of the wireless infrastructure necessary for the completion of the call. The priority must begin at the wireless terminal for network access, continue through the wireless network to the terrestrial public switched network (if required), and through the terminating end (egress) for end-to-end wireless call completion. Priority Service must include the ability to invoke Government Emergency Telecommunications Service (GETS) from the wireless network.

## **6.9.2 Telecommunications Service Priority (TSP) and GETS**

The TSP System is the regulatory, administrative and operational system that provides for priority treatment (i.e., provisioning and restoration) of national security and emergency preparedness (NS/EP) telecommunications services. NS/EP telecommunications services are those critical to maintaining a state of readiness for, responding to or managing telecommunications during an event or crisis that could cause harm to the population, damage property, or threaten the security of the United States. The TSP System is the only authorized mechanism for receiving priority provisioning and restoration of NS/EP telecommunications services.

TSP ensures priority treatment for the Nation's most important telecommunications services—those that serve our national security leadership; national security posture and U.S. population warning; public health, safety and maintenance of law and order; and public welfare and maintenance of the national economic posture.

TSP supports response to natural disasters and civil and military crises, emergency communications networks and Federal Government functions such as Presidential travel and visits by foreign dignitaries.

State, local and foreign governments and private industry may be sponsored by a Federal organization to obtain TSP restoration or provisioning priority.

GETS is the communications service that enhances the call access, transport and egress with a nationwide switched voice and low speed data capabilities by utilizing the surviving PSTN resources. GETS calls are afforded priority treatment and enhanced routing in the PSTN. GETS, which is available nationwide, provides domestic and (some) international access and egress. User authorization is provided using personal identification numbers (PIN) assigned to the authorized users. A new industry standard for the identification of priority calls as they travel through the PSTN has been approved in the standards arena and is known as High Probability of Completion (HPC). The HPC definition resides in the call signaling of the authorized user and facilitates priority treatment and specialized routing services implemented by the GETS program.

## **6.10 Security**

**6.10.1 General** - In addition to the inherent security challenges of radio communications, wireless communications provides an entry point into a global information infrastructure consisting of all types of Information Technology transmission, processing and storage systems. Wireless systems must be viewed as a communications system that is an integral part of the global information technology infrastructure. The Federal Government therefore must also consider the systems level security ramifications of wireless technology and not just the radio and Public Network issues considered in the past. The wireless security paradigm must also take into account the security ramifications of wireless access into virtual private networks, public data networks and databases, signaling systems, and local area networks.

**6.10.2 Threat to Wireless Systems** - Threat is defined as the motivation and capability of an adversary. In making decisions about the security services required by the system, it is important to address not only present threats but also threats projected throughout the life of the system. Threat must be addressed at the architectural level, when identifying what security services will be included and the assurance level of those services. (The "Federal User Wireless Telephone Security Risks" available at [www.nist.gov/fwuf](http://www.nist.gov/fwuf) documents the status of risks and recommendations today for cellular systems.) The

following lists examples of potential attacks against modern wireless systems and is not intended to be comprehensive.

- Passive intercept attacks against control signals
- Passive intercept attacks against user signals
- Active attacks against wireless network including those network functions involved in:
  - security service management
  - security mechanism management
  - security audit
  - security recovery
  - coordination of network security services
  - intersystem messaging security
- Physical attacks against the mobile unit
- Geolocation
- Jamming
- Spoofing
- Denial of Service
- Attacks against the security management infrastructure that provides user authentication data, passwords, keys, authentication algorithms, etc.
- Passive and active attacks against IT infrastructure using wireless technology

### **6.10.3 Federal Security Service Requirements**

Federal user requirements include many security services that are common to the normal business user and should be available as part of the wireless network. Additional requirements beyond those available from the network depend on the value of the information and on the threat environment.

In general, there are three tiers of security requirements for the federal user. The first tier consists of security services that are provided by the network and can be utilized as a commercial service. This covers the majority of federal applications. The second tier requirements consist of special devices that are added-on to the mobile unit to provide the additional security services required for special government functions. This covers the many federal missions where enhanced products such as NSA's CONDOR secure handsets are needed. The third tier services use commercial network components to create a real or a virtual private network, to provide custom services. This includes the public safety and military applications where private networks are commonly used.

The following security services can be identified with requirements associated with three tiers in the table below:

- a) Confidentiality – the protection of user data, signaling, identification, and location
- b) Integrity – the protection from insertion, deletion, modification, or replay of data.

- c) System availability – ability to obtain access to the service and the prevention of accidental or malicious denial of service
- d) Authentication – the assured identification of the user, terminal, and carrier
- e) Accountability – the ability to verify transactions

While each service is normally defined separately, in practice, they are neither isolated nor independent of each other; each service interacts with and depends on the others. New policies might be needed to provide wireless users with guidelines of processing classified information/having classified discussions outside areas approved for classified processing (i.e., while in transit or at a non-office environment).

Table 1: Security Service Requirement by Tier

<b>Security Service Provided by:</b>	<b>Tier 1 Carrier</b>	<b>Tier 2 User Terminal</b>	<b>Tier 3 Private Network</b>
<b>Confidentiality</b>			
Data Content	X	X	X
Data content- stored	X	X	X
Signaling			X
Detection			X
Identification	X	X	X
Geolocation	X	X	X
<b>Integrity</b>			
Insertion of transmitted data	X	X	X
Deletion of transmitted data	X	X	X
Modification of stored data	X	X	X
Replay of data		X	X
<b>Authentication</b>			
Mobile to Mobile		X	X
Mobile to/from Network	X	X	X
User to Mobile unit		X	X
<b>Availability</b>			
Emergency Restoration	X	X	X
Accidental Denial	X	X	X
Malicious Denial		X	X
Priority Access	X	X	X
Priority Egress	X	X	X
<b>Non-repudiation</b>			
Mobile to network manager	X	X	X
Mobile to Mobile		X	X
Mobile to/from network manager		X	X

For Tier 2 and Tier 3 security services to be implemented in a cost-effective manner, the Federal Government requires the following:

- a. Both the infrastructure and the mobile units shall allow for the ability to overlay end-to-end encryption.
- b. Infrastructure and mobile units shall allow for access to government security management infrastructure or commercial public key infrastructures in a manner that is transparent to the user.
- c. Standards shall be clearly defined; unambiguous so that “optional” fields in protocols can be used to invoke government or industry unique services

- d. Published security policies (best commercial practices) used within a carrier's network and between carrier elements.
- e. Seamless handoff so that the mobile unit and base station do not lose bit count integrity.
- f. Certification of commercial security services using the common criteria through a National Information Assurance Program (NIAP) certified testing facility when available

## **7.0 Spectrum Issues**

If the government users of wireless are limited to dedicated use of government allocated frequencies for government required services, then a larger allotment of spectrum will be required than currently exists. If government users are expected to share networks with commercial users as part of a network sharing agreement, these networks will be required to accommodate priority service schemes. This may be accommodated through separate or combined use of the services and features discussed. Any sharing of services between government and commercial users would require that some combination of these services or features be an inherent part of wireless standards. Failure to accommodate some combination of these services or features into wireless would severely inhibit emergency services. If the government user is to share spectrum and services with commercial users, the requirements described in this document must be satisfied.

Federal user requirements may be accommodated by a variety of communication system applications. A solution for overall accommodation of federal requirements may include one or more of the following approaches.

- Use of commercial services by lease or subscription
- Use of wireless frequencies as a secondary government allocation to a primary non-government mobile application.
- The use of government owned or leased systems on government frequencies.

The federal users need more than just voice service in one small region. Federal users require a minimum set of voice and data services that must inter-operate across technologies, networks, carriers, and media boundaries. These services must be defined and supported by industry standards bodies to provide the federal user with DUTS capability.

If the government is to share spectrum with commercial users, the government may need to operate in bands for unlicensed services with commercial users. This would include both the government use of government owned commercial unlicensed (type accepted) equipment as well as modified commercial equipment to support government/military

unique features such as (unlicensed) PBX's in government facilities or modified commercial wireless LAN equipment for military tactical applications.

Government services in a shared spectrum environment must be supported during restoration procedures in the event of disaster. Restoration of commercial services may be supplemented by importing government radio systems on government frequencies.

The increased dependency of the U.S. military on commercial wireless devices and services requires new approaches for provisioning services where available and spectrum for real or virtual private systems deploy nationally and internationally.

## GLOSSARY

CAS - Call Associated Signaling  
CIO - Chief Information Officer  
COTS - Commercial Off-The-Shelf  
DUIITS - Digital, Ubiquitous, Interoperable, Transparent, and Secure  
EMI/EMC - Electromagnetic Interference and Compatibility  
FWPC - Federal Wireless Policy Committee  
FWUF - Federal Wireless Users Forum  
GETS - Government Emergency Telecommunications Service  
HPC - High Probability of Completion  
MSS - Mobile Satellite Service  
NCAS - Non-Call Associated Signaling  
NS/EP - National Security And Emergency Preparedness  
NSA - National Security Agency  
NSTAC - National Security Telecommunications Advisory Committee  
NTIA - National Telecommunications and Information Administration  
OMNCS - Office of the Manager, National Communication System  
PBX - Wireless Private Branch Exchange  
PCS - Personal Communications Systems  
PIN - Personal Identification Numbers  
SMR - Specialized Mobile Radio  
TSP - Telecommunications Service Priority  
UIM - User Identity Module  
WLAN - Wireless Local Area Network  
WLL - Wireless local loop  
WWAN - Wireless Wide Area Networks